REMARKS

Claims 1-83 are now pending in the application. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

Applicant would like to thank the Examiner for courtesy extended during the interview on October 11, 2007.

REJECTION UNDER 35 U.S.C. § 103

Claims 1-21, 23-79, and 81-83 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims III (U.S. Pat. No. 6,550,011 B1) in view of Tai et al. (U.S. Pat. No. 2004/0034785A1). This rejection is respectfully traversed.

With respect to Claim 1, Applicant submits that Sims III and Tai do not at least show, teach or suggest decryption of an encrypted content key using a private key that is generated based on a device specific identification (ID). The private key is used by a public key decryption module to decrypt an encrypted content key. Note that the private key is not used to decrypt encrypted content, but rather is used to provide a content key for such decryption.

As Claim 1 recites a public key decryption module for a hard-disk drive that encrypts a content key, Claim 1 is directed to distributed content. This is consistent with the specification of the present application. In a distributed content environment, the content is encrypted prior to reception by an end user. The end user decrypts the content based on a received content key and a public/private key combination.

The Examiner admits that Sims III fails to disclose a private key that is generated based on a device specific ID. For at least this reason, Sims III also fails to disclose decryption of an encrypted content key using a private key that is generated via a device specific ID.

The Examiner alleges that Tai discloses a private key that is generated via a device specific ID. Applicant submits that the private key of Tai is substantially different and is used differently than a disclosed device secret key of Sims III and the private key of Claim 1.

As best understood by Applicant, Sims III is directed to security of distributed content and discloses a device secret key that is used to decrypt a content key. The content key is used to decrypt distributed content. As an example, distributed content may include digital music that is transmitted from a distributor to end users.

In contrast, Tai is directed to security of boot-up software that is transferred between memories of a device. Tai discloses a private key that is used to encrypt boot-up software of a device. The boot-up software is locally stored on the device and is not distributed.

As best understood by Applicant, Tai discloses a device that includes ROM and a controller with RAM. Boot-up software is stored in the ROM. Tai states that upon an initial power up of the controller at an end product manufacturing site, the controller downloads the boot-up software from the ROM to the RAM. The controller encrypts the boot-up software using a 64-bit number that is based on a chip's die ID number. Once encrypted, the boot-up software is up-loaded and stored on the ROM for future use. In other words, the boot-up software is encrypted at the manufacturing site and stored on

the ROM prior to the corresponding computer system being delivered to an end user. Once the end user receives the computer system, the software is already encrypted and is simply decrypted for use by the same controller.

Thus, this encryption of Tai occurs once and is directed to boot-up software that is stored on an onboard memory of a device and that remains on that onboard memory. Tai is not directed to digital content that is distributed by a content distributor over a network or the Internet to end users. For this reason Tai does not use content keys and/or private/public key combinations. Therefore, Tai does not disclose decryption of an encrypted content key using a private key that is generated via a device specific ID.

It is a longstanding rule that to establish a prima facie case of obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 180 USPQ 143 (CCPA 1974), see M.P.E.P. §2143.03. Claim 1 is allowable for at least the above reasons.

Since there is no relationship between the device secret key of Sims III and the private key of Tai, there would be no reason to combine and/or modify the decryption techniques of Sims III using a private key for encryption of a boot-up software. In Sims III, the media content is encrypted prior to being distributed to end users. On the other hand, in Tai boot-up software is locally and internally encrypted and stored. The boot-up software is not distributed or provided to multiple end users. Thus, the protection techniques between Sims III and Tai are different.

One cannot simply replace the private key of Tai with the device secret key of Sims III, as the keys are used for different applications. The private key of Tai is used

for encryption of boot-up software and the device secret key of Sims III is used for the decryption of an encrypted content key. See col. 13, lines 43-44 of Sims III for disclosure and use of the device secret key. Thus, it is improper to combine the teachings of Sims III and Tai.

Claim 1 is further novel and nonobvious for at least the above reasons.

Therefore, Claim 1 is allowable for at least the above reasons. Claims 20, 31, 50 and 61 are allowable for at least similar reasons. Claims 2-19, 21-30, 32-49, 51-60 and 62-83 ultimately depend from Claims 1, 20, 31, 50 and 61 and are allowable for at least similar reasons.

With respect to Claim 10, the Examiner alleges that Sims III and Tai disclose a public key decryption module that performs digital signature verification of a content directory entry corresponding to content that is selected for play. The Examiner refers to col. 15, line 48 and to col. 17, line 25 of Sims III for such disclosure. Applicant traverses.

In col. 15, lines 46-49, Sims III discloses encryption of content use information in order to protect the information from unauthorized alterations. In col. 17, lines 23-27, Sims discloses the comparing of a public key to content use information to determine if a device is authorized to receive content. The stated sections do not disclose signature verification of a content directory corresponding to content that is selected for play. Applicant is unable to find disclosure of this feature anywhere in Sims III.

Thus, Claim 10 is further novel and nonobvious for at least the above reasons.

With respect to Claim 11, the Examiner alleges that Sims III and Tai disclose a content directory entry that contains a clear content counter that specifies a portion of a corresponding content that is not encrypted. The Examiner refers to col. 15, line 7 of Sims III for such disclosure. Applicant traverses.

In col. 15, lines 5-7, Sims III discloses copy management rules that include allow playback times. In other words, Sims III discloses content use information that includes the number of playback iterations permitted. Sims III also appears to disclose content information that includes when to delete content. The stated information is unrelated to what content is encrypted. Knowledge of a number of permitted playbacks and when content should be deleted does not suggest what portion of content is or is not encrypted.

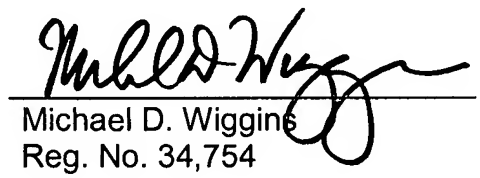
Thus, Claim 11 is further novel and nonobvious for at least the above reasons.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action and the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: November 15, 2007

By: 

Michael D. Wiggins
Reg. No. 34,754

Jeffrey J. Chapp
Reg. No. 50,579

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

MDW/JJC/mrg